IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Schaeck et al.	Confirmation No.:	1249
Serial No.:	09/731,509	Group Art Unit:	2136
Filed:	12/07/2000	Examiner:	Colin, Carl G.
Title:	CONDITIONAL SUPPRESSION OF CARD HOLDER VERIFICATION		

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being electronically transmitted to: Mail Stop Appeal Briefs – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on January 21, 2009.

Rosalind Q. Spiller

Rosalind Q. Spiller

Date of Signature: January 21, 2009.

To: Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

APPELLANTS' REPLY BRIEF TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Dear Sir:

In reply to the Examiner's Answer mailed on November 20, 2008, Appellants submit this Reply Brief under 37 C.F.R. 41.41. It should be noted that this Reply is being filed under the rules in effect prior to December 10, 2008, the new rules having been delayed as of this filing. Any Reply Brief is due by January 21, 2009 (January 20, 2009 was the presidential inauguration and the U.S. Patent and Trademark Office was closed). Therefore, this Reply Brief is being timely filed.

ARGUMENT

Issue No. 1

With regard to the performing aspect of claim 16, the Answer apparently alleges that card holder verification in Rikuna is done "without a holder of the card providing information" as claimed. However, it is clear from Rikuna that user verification is always done by the card holder either entering their PIN into the remote PIN entry card 21, or, if the other card (card 11) is directly connected to the terminal, the card holder enters his PIN directly into the terminal. In other words, the holder of the card is always providing information by providing their PIN each time. See Rikuna at, for example, column 6, lines 8-11 and step A3 in FIG. 6 of Rikuna, as well as column 9, lines 30-33. PIN entry by the card holder as part of card holder verification (Rikuna column 9, lines 11-12) is further confirmed by step B13 in FIG. 7B, described at column 8, lines 30-32. See also Rikuna at column 8, lines 64-66.

Further, the objects of the invention language from Rikuna quoted in the Answer itself confirms saving the customer in the main embodiment from physically having to go to the terminal to enter their PIN by use of the remote PIN entry card, which is done with each use. Indeed, even the title of Rikuna indicates a purpose of allowing remote PIN entry, but PIN entry for card holder verification nonetheless.

The Answer apparently alleges that since the card holder in Rikuna may enter the PIN in the remote PIN entry card before it is taken by the waitress, somehow the card holder is not proving information for card holder verification. Appellants submit there is no express or implied time frame for card holder verification in claim 16, such that any time lag in the scenario

of Rikuna between when the PIN is entered and the PIN being used for verification is simply not relevant.

The performing aspect of claim 16 has at least the following limitations to keep in mind when parsed: (1) another identifier is provided to the card from the device; (2) the card is the same card that was used for checking the trusted association; (3) the another identifier is for comparing by the card to a second identifier stored on the card; and (4) the second identifier stored on the card is different from the first identifier stored on the card that was used to check for a trusted association.

In contrast, the cited Rikuna scenario is as follows: the card holder enters his PIN into remote PIN entry card 21; the card is inserted into terminal 12 and the PIN is transferred by the terminal to card 11, which is a different card from card 21; the PIN transferred is the same PIN that was entered by the card holder; card 11 (not card 21) compares the transferred PIN to a PIN previously stored on card 11.

Appellants submit that comparing the performing aspect as parsed above to Rikuna reveals at least the following differences. The PIN in Rikuna is not provided to the original card storing the PIN (card 21), but to a different card (card 11). Claim 16 calls for the same card. The PIN provided to the different card is the same PIN originally stored on card 21; it is the PIN originally input by the card holder. However, the claim calls for an identifier different from the first identifier stored on the card.

Appellants submit that Nakanura and the alleged combination fail to remedy the shortcomings of Rikuna noted above and in the Appeal Brief.

Finally, against the aspect of claim 16 of involving the card holder in verification if there is no trusted association, the Answer cites to the embodiment of Nakamura where a PIN is required only if the transaction amount exceeds a preselected floor. However, Appellants submit that Rikuna and Nakamura are at odds in this regard, since Rikuna always requires PIN entry by the card holder, while Nakamura does not. Indeed, the main point of Rikuna is to eliminate the need for the card holder to go to the terminal to enter a PIN, but not to eliminate the PIN altogether. Thus, Appellants submit the teachings are at odds, such that one skilled in the art would not combine Nakamura with Rikuna as alleged in the Answer. Moreover, Appellants submit not requiring a PIN for a transaction amount lower than a set amount is not the same as requiring a trusted association; rather, it is a decision not to check for a trusted association at all below the set amount, and instead simply assuming the risk of fraud at that level.

Appellants submit that Rikuna and the alleged combination fail to remedy the shortcomings of Nakamura noted above and in the Appeal Brief.

Therefore, for at least the reasons noted above and in the Appeal Brief, Appellants submit that claim 16 is not obvious over Rikuna in view of Nakamura.

With regard to the claim 33 aspect where there is no trusted association, the Answer alleges that Rikuna discloses PIN comparison done in the card. However, regardless of whether the allegation is true, the PIN entered by the card holder is recited in claim 33 as being compared

by the card to a *second* identifier stored on the card. Note that the first identifier stored on the card was used to check for a trusted association between the card and the terminal. In the scenario described at the bottom of page 22 of the Answer regarding Rikuna (column 9, line 26+), there is no determination of a lack of a trusted association prior to PIN entry and comparison.

Appellants submit that Nakamura and the alleged combination fail to remedy the shortcomings of Rikuna noted above and in the Appeal Brief.

Therefore, for at least the reasons noted above and in the Appeal Brief, as well as the above comments with respect to claim 16 for similar aspects, Appellants submit that claim 33 is not obvious over Rikuna in view of Nakamura.

With regard to claim 20, the Answer apparently again argues the alleged timing distinction to which Appellants do not acquiesce. Nonetheless, the fact remains that the card holder provides the PIN in card 21 that is used for verification by card 11 after transfer with an unavoidable delay between entry and comparison, which is necessitated by the two-card process of Rikuna.

Appellants submit that Nakamura and the alleged combination fail to remedy the shortcomings of Rikuna noted above and in the Appeal Brief.

Therefore, for at least the reasons noted above and in the Appeal Brief, Appellants submit that claim 20 is not obvious over Rikuna in view of Nakamura.

With regard to claim 29, the Answer now cites to Rikuna at column 4, lines 22-27. However, even if for the sake of argument, it were assumed that storing a terminal ID creates an association, the fact remains that Rikuna teaches a two-card system, the main card and the remote PIN entry card. The argument in the Answer speaks to only one card, the main card. Appellants submit there is no teaching or suggestion in Rikuna regarding creating an association between the remote PIN entry card and the terminal. Thus, since in effect the Answer reads the two cards of Rikuna on the one card of the present claims, it stands to reason that both cards would need to have an association with the terminal to properly read on claim 29, but such teaching is not present in Rikuna.

Appellants submit that Nakamura and the alleged combination fail to remedy the shortcomings of Rikuna noted above and in the Appeal Brief.

Therefore, for at least the reasons noted above and in the Appeal Brief, Appellants submit that claim 29 is not obvious over Rikuna in view of Nakamura.

Regarding claim 30, the Answer alleges that checking to see whether the terminal and card in Rikuna are compatible using the terminal identification code (TID) constitutes controlling the association. However, even ignoring the association aspect (see claim 29 from which claim 30 depends), Appellants respectfully disagree. While checking compatibility may determine whether the card and terminal are operable together, such checking cannot reasonably be said to control anything, let alone the association. It is merely information. Moreover, the Answer already argued that storing the TID on the card creates the association. See the Answer at page 24 with respect to claim 29. The Answer also indicates that the TID is stored before the

terminal/card operability check. Thus, the alleged association is made, prior to and uncontrolled by the outcome of the operability check.

Appellants submit that Nakamura and the alleged combination fail to remedy the shortcomings of Rikuna noted above and in the Appeal Brief.

Therefore, for at least the reasons noted above and in the Appeal Brief, Appellants submit that claim 30 is not obvious over Rikuna in view of Nakamura.

Issue No. 2

With regard to claim 24, the Answer alleges that erasing the PIN in Risafi constitutes erasing the association between the PIN and the card identifier. However, Appellants submit that the PIN and the association are simply two different things, and the claim recites erasing the association, not erasing the PIN. As just one indication of how they are different, as mentioned in the Appeal Brief, erasing the association does not affect the PIN number itself.

Appellants submit that neither Rikuna nor Nakamura, nor the alleged combination thereof, remedies the shortcomings of Risafi noted above and in the Appeal Brief.

Therefore, for at least the reasons noted above and in the Appeal Brief, Appellants submit that claim 24 is not obvious over Rikuna in view of Nakamura and Risafi.

CONCLUSION

In conclusion, Appellants submit that claims 16-20, 22, 25, 28-36 are not obvious over Rikuna (U.S. Patent No. 4,752,678) in view of Nakamura et al. (U.S. Patent No. 5,917,168), and that claims 23-24 and 26-27 are not obvious over Rikuna in view of Nakamura et al. (U.S. Patent No. 5,917,168) as applied to claims 16, 22 and 25, and further in view of Risafi et al. (U.S. Patent No. 6,473,500). Therefore, Appellants continue to submit that the final Office Action should be reversed in all respects.

Wayne F. Reinke
Attorney for Appellants
Registration No.: 36,650

Dated: January 21, 2009.

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 Columbia Circle
Albany, New York 12203-5160
Telephone: (518) 452-5600
Facsimile: (518) 452-5579